MICHAEL R. REESE (Cal. SBN 206773)
mreese@reesellp.com
SUE J. NAM (Cal. SBN 206729)
snam@reesellp.com
REESE LLP
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

GEORGE V. GRANADE (Cal. SBN 316050)
ggranade@reesellp.com
8484 Wilshire Boulevard, Suite 515
REESE LLP
Los Angeles, California 90211
Telephone: (310) 393-0070

CALEB MARKER (Cal. SBN 269721)
caleb.marker@zimmreed.com
ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, California 90048
Telephone: (877) 500-8780

BRIAN C. GUDMUNDSON (to be admitted *pro hac vice*)
brian.gudmundson@zimmreed.com
RACHEL K. TACK (to be admitted *pro hac vice*)
rachel.tack@zimmreed.com
MICHAEL J. LAIRD (to be admitted *pro hac vice*)
michael.laird@zimmreed.com
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400

Attorneys For Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

JOSHUA KELLER, on behalf of himself and all others similarly situated, Plaintiff, v. CHEGG, INC., Defendant.	CASE NO.: 22-cv-6986 **COMPLAINT** **CLASS ACTION** **Jury Trial Demanded**

Plaintiff Joshua Keller ("Plaintiff"), by his undersigned counsel, files this Class Action Complaint on behalf of himself and a class of all similarly situated persons against Defendant Chegg, Inc. ("Chegg" or "Defendant"). Plaintiff bases the forgoing allegations upon personal information and belief, the investigation of counsel, and states the following:

INTRODUCTION

1. Chegg markets and sells direct-to-student educational products and services.[1] This includes renting textbooks, guiding customers in their search for scholarships, and offering online tutoring.[2] Chegg claims it "strive[s] to improve the overall return on investment in education by helping students learn more in less time and at a lower cost."[3] The company also claims to bring "integrity to [its] products, customers, work environment, and the community."[4] According to Chegg, the target audience for its services and products are primarily high school and college students.

2. Since approximately September 2107, Chegg experienced, at least, four data security breaches: (1) September 2017; (2) April 2018; (3) April 2019; and (4) April 2020 (collectively the "Data Breaches").

3. The first data breach occurred in September 2017, when multiple Chegg employees fell for a phishing attack that allowed a hacker to gain access to employees' direct deposit information. Upon information and belief, this breach was limited to the exposure of employee data.

4. Approximately seven months later, in April 2018, a former Chegg contractor used login information the company shared with employees and contractors to access one of Chegg's third-party cloud databases, resulting in the exposure of millions of customers' personal information. According to the Federal Trade Commission ("FTC"), Chegg allowed employees and third-party contractors to access Amazon-hosted storage with a single access key that provided full administrative privileges over all

[1] *Multiple data breaches suggest ed tech company Chegg didn't do its homework, alleges FTC*, Leslie Fair, Federal Trade Commission, Oct. 31, 2022: *https://www.ftc.gov/business-guidance/blog/2022/10/multiple-data-breaches-suggest-ed-tech-company-chegg-didnt-do-its-homework-alleges-ftc* (last visited Nov. 4, 2022).
[2] *Id.*
[3] *Id.*
[4] *Id.*

information.[5] The April 2018 data breach exposed the personal information of approximately forty (40) million customers. The exposed personal information included names, email addresses, passwords, and for certain users, sensitive scholarship information such as dates of birth, parents' income range, sexual orientation, and disabilities. Upon information and belief, this breach exposed both consumer and employee data.

5. In September 2018, a threat intelligence vendor informed Chegg that a file containing some of this exfiltrated information was available in an online forum.[6] Chegg reviewed the file as part of its own investigation, finding it held, among other things, approximately 25 million of the exfiltrated customers' passwords, from the April 2018 breach, in plain text, meaning the threat actors had cracked the hash for those passwords.[7] Chegg required approximately 40 million Chegg platform users to reset their passwords.[8] Even after this, Chegg continued to store consumer personal information in plain text.[9]

6. The third breach, in April 2019, was the result of another phishing attack, giving hackers access to a Chegg executive's email inbox, which contained personal information of Chegg users and employees, including financial and medical data.[10] Upon information and belief, this breach exposed both consumer and employee data.

7. And most recently, the fourth data breach in April 2020, exposed W-2 information, including birth dates and Social Security numbers for approximately 700 current and former employees.[11] Upon information and belief, this data breach was limited to the exposure of employee data.

8. From September 2017 through April 2020, Chegg did not make reasonable modifications to its data security, including an egregious failure to implement any phishing attack training for its employees. It also did not implement a written data security policy until January 2021.

---

[5] *FTC schools edtech giant Chegg over 'careless' cybersecurity practices*, Carly Page, Join TechCrunch+, Nov. 1, 2022: https://techcrunch.com/2022/11/01/ftc-chegg-breaches-cybersecurity/, (last visited Nov. 7, 2022).
[6] *In the Matter of CHEGG, INC., a corporation*, (last visited, Nov. 7, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2023151-Chegg-Complaint.pdf.
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*

9. On October 31, 2022, the FTC filed a complaint accusing Chegg of numerous cybersecurity lapses that resulted in the four data breach between 2017 and 2020.[12] Upon information and belief, this was the first public notice of the breaches.

10. According to the FTC, these data breaches were the result of "poor data security practices, including the use of single login for all compromised databases, a lack of multi-factor authentication, the storing of all users' and employee's data in plaintext, and a failure to monitor networks for malicious activity.[13] Indeed, Chegg did not have a written security policy until January 2021.[14] Failure to implement these basic data security practices violates standard practice and is wholly unreasonable.

11. Plaintiff therefore brings this Class Action Complaint seeking relief for his injuries and those of persons who were similarly impacted by the Data Breaches and Chegg's inadequate data security.

JURISDICTION

12. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005. Subject matter jurisdiction is proper because: (1) the amount in controversy in this class action exceeds five million dollars ($5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendants; and (4) the Defendant is not a government entity.

13. This Court has general personal jurisdiction over Chegg because Chegg is headquartered and operates its principal place of business in Santa Clara, California. Chegg has minimum contacts with California because it is located there and conducts substantial business there, and Plaintiff's claims arise from Chegg's conduct in California.

14. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in California and because Chegg conducts a substantial part of its business within this District.

---

[12] *FTC schools edtech giant Chegg over 'careless' cybersecurity practices*, *supra* note 5.
[13] *Id.*
[14] *Id.*

PARTIES

15. **Plaintiff** Joshua Keller is a resident of Hillsborough, California. He used Chegg's services throughout his high school and college education, including for exam, homework, and project help. Plaintiff has been a Chegg customer for approximately the last six years. Plaintiff reasonably believes his data was compromised by the Chegg Data Breaches. After these data breaches and specifically over the last two months, Plaintiff experienced identity theft and fraud, including multiple credit checks initiated on his behalf and a credit card issued in his name, both without his authorization or consent. Plaintiff has spent time and effort with his bank dealing with this credit card fraud. He also noticed an increase in spam calls and emails and spent time and effort changing multiple passwords to his various subscriptions or accounts. Plaintiff reasonably believes that all of this, the identity theft and fraud and the increase in spam, is a direct and proximate result of the Chegg Data Breaches, particularly because this fraud all occurred after the Data Breach and Plaintiff does not reasonably believe it could be related to any other event.

16. **Defendant** Chegg is a Delaware limited liability company with its headquarters and principal place of businesses in Santa Clara, California.

BACKGROUND

A. Chegg Collects Sensitive Information from Users

17. In providing its services and for employment, Chegg collects sensitive personal information from customers. This information includes name, email address, username, password, demographic, school, gender, age or birthdate, zip or postal code, photographs, information about academic and work history, phone number, mailing address, and information about interests and preferences.[15]

18. If a user requests information about Chegg's scholarship services, the user is directed to update their profile. The additional information Chegg collects here includes a customer's religious denomination, heritage, date of birth, parents' income range, sexual orientation, military affiliations,

[15] *Privacy Policy*, (last visited, Nov. 7, 2022), https://www.chegg.com/en-US/privacypolicy.

citizenships, disabilities, interests, and participation in clubs and sports (collectively, the "Scholarship Search Data").[16] This data is highly sensitive.

19. As another example, in connection with its online tutoring services, Chegg records videos of tutoring sessions that include Chegg users' likeness, images, and voices. Again, this is highly sensitive information.

20. Chegg also collects information automatically when users use the services, including internet protocol (IP) address, user setting, MAC address, cookie identifies, mobile carrier mobile advertising and other unique identifies, details about users' browser, operating system or device, location information, Internet or mobile service provider, pages that users visit before, during, and after using the services, information about links users click, and other information about how users use Chegg's services.[17]

21. Taken together, these paragraphs, collectively and independently identify "Sensitive Information."

B. Chegg's Inadequate Data Security Measures Exposed Customers' Sensitive Information

22. As part of its information technology infrastructure, Chegg uses a third-party service provided by Amazon Web Services called the Simple Storage Service ("S3"). S3 is a scalable cloud storage service that can be used to store and retrieve large amounts of data. The S3 stores data inside virtual containers, called "buckets," against which individual access controls can be applied. [18]

23. Chegg relies on S3 buckets to store a wide variety of files that contain customers' sensitive personal information, including their names, passwords, dates of birth, and Scholarship Search Data.[19]

24. From at least 2017 to the 2020, Chegg has engaged in several practices that failed to provide reasonable security to prevent unauthorized access to customers' personal information. Among other things, Chegg:

[16] *Profile Info*,(last visited, Nov. 7, 2022), https://www.chegg.com/my/profile.
[17] *Privacy Policy*, *supra* note 7.
[18] *In the Matter of CHEGG, INC., a corporation*, *supra* note 6.
[19] *Id.*

a) failed to implement reasonable access controls to safeguard users' personal information stored in S3 databases until at least October 2018. Specifically, Chegg:

i) failed to require employees and third-party contractors that access the S3 databases to use distinct access keys, instead permitting employees and contractors to use a single AWS access key that provided full administrative privileges over all data in the S3 databases ("AWS Root Credentials");

ii) failed to restrict access to systems based on employees' or contractors' job functions;

iii) failed to require multi-factor authentication for account access to the S3 databases; and

iv) failed to rotate access keys to the S3 databases;

b) stored users' and employees' personal information on Chegg's network and databases, including S3 databases, in plain text, rather than encrypting the information;

c) used outdated and unsecure cryptographic hash functions to protect users' passwords;

d) failed to provide adequate guidance or training for employees or third-party contractors regarding information security and safeguarding users' and employees' personal information, including, but not limited to, failing to require employees to complete any data security training;

e) failed to develop, implement, or maintain adequate written organizational information security standards, policies, procedures, or practices;

f) failed to have a policy, process, or procedure for inventorying and deleting users' and employees' personal information stored on Chegg's network after that information is no longer necessary; and

g) failed to adequately monitor its networks and systems for unauthorized attempts to transfer or exfiltrate users' and employees' personal information outside of Chegg's network boundaries.[20]

C. Chegg's Inadequate Data Security Caused Multiple Data Breaches

25. Chegg's failure to provide reasonable data security for the Sensitive Information it collected from customers has led to the repeated exposure of that personal information.

26. In approximately September 2017, Chegg employees fell for a phishing attack, giving the threat actors access to employees' direct deposit information. Prior to the hack, Chegg did not require employees to complete any data security training, including identifying and appropriately responding to phishing attacks; this failure contributed to the security incident.

27. Seven months later, in April 2018, a former contractor accessed one of Chegg's S3 databases using an AWS Root Credential. Although Amazon had provided public guidance to protect

[20] *In the Matter of CHEGG, INC., a corporation*, *supra* note 6.

AWS Root Credentials "like you would your credit card numbers or any other sensitive secret" and that Amazon "strongly recommend[s] that you do not use the root user for your everyday tasks, even the administrative ones," Chegg shared the AWS Root Credentials among its employees and even outside contractors.[21] The former contractor exfiltrated a database containing personal information of approximately 40 million Chegg customers.

28. The exposed personal information included users' email addresses, first and last names, passwords, religious denomination, heritage, date of birth, parents' income range, sexual orientation, and disabilities. Chegg encrypted users' passwords using an outdated function that had been criticized by experts for years prior to April 2018.[22] Had Chegg employed reasonable access controls and monitoring, it would have likely detected and/or stopped the attack more quickly.

29. In approximately April 2019, a senior Chegg executive fell for a phishing attack, giving a hacker access to the executive's credentials to Chegg's email platform and exposing personal information about consumers and employees of Chegg. This executive's email system was in a default configuration state that allowed employees, as well as threat actors, to bypass Chegg's multifactor authentication requirement while accessing the email platform. The threat actor exploited this shortfall and gained access to the executive's email inbox, which contained the personal information of Chegg users and employees, including their financial and medical information.[23]

30. Had Chegg properly configured its systems, including requiring multifactor authentication for employees to access their emails, this phishing attack, and the resulting exposure of consumer Sensitive Information, could have been prevented.

31. In addition, Chegg's failure to require employees to complete any data security training, including training to identify and respond to phishing attacks, contributed to the security incident.

32. Most recently, in April 2020, Chegg's senior employee responsible for payroll fell for a phishing attack, giving the threat actor access to the employee's credentials to Chegg's payroll system. The threat actor exfiltrated the W-2 information, including the birthdates and Social Security numbers,

---

[21] *In the Matter of CHEGG, INC., a corporation*, *supra* note 6.
[22] *Id.*
[23] *Id.*

of approximately 700 current and former employees. Despite Chegg employees falling for phishing attacks on at least two prior occasions, Chegg still did not require, in or before April 2020, its employees to complete any data security training, including identifying and appropriately responding to phishing attacks.[24]

D. Chegg Knew It Needed to Protect Customers' Sensitive Information

33. Chegg knew the user data it collected and stored in connection with its services was highly sensitive.

34. From approximately March 2017 to January 2020, Chegg's privacy policy included the following language: "Chegg takes commercially reasonable security measures to protect the Personal Information submitted to us, both during transmission and once we receive it."[25] From January 2020 to the present, Chegg's privacy policy contained the following statement concerning that same personal information: "We take steps to ensure that your information is treated securely and in accordance with this Privacy Policy."[26] These statements indicate that Chegg was aware the sensitive and personal nature of the user data it stored.

35. Additionally, in a February 7, 2022 Press Release, Chegg included some "Forward Looking Statements." Within those statements, Chegg mentioned service disruptions related to cybersecurity and cyber-attacks twice throughout the statement, indicating that it was aware the potential for such threats.[27]

E. Plaintiff's and the Class's Sensitive Information Has Value.

36. The personal, health, and financial information of Plaintiff and the Class is valuable, intangible property. Indeed, it has market value to advertisers and cybercriminals seeking to obtain and use that information and the public and the marketplace values maintaining the privacy and

[24] *In the Matter of CHEGG, INC., a corporation*, *supra* note 6.
[25] *Id.*
[26] *Id.*
[27] *Chegg Investor Relations*, (last visited Nov. 7, 2022), https://investor.chegg.com/Press-Releases/press-release-details/2022/Chegg-Reports-2021-Financial-Results-and-Gives-2022-Guidance/default.aspx.

confidentiality of individuals' Sensitive Information. Thus, Chegg was on notice of the need to implement reasonable data security measures.

37. Unlike financial information, like credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. For these reasons, these types of information are the most lucrative and valuable to hackers.[28]

38. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on an ongoing basis rather than exploiting just one account until it's canceled.[29]

39. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[30] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[31]

40. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[32]

41. Consumers and businesses also place a considerable value on maintaining the privacy and confidentiality of their Sensitive Information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between

---

[28] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, (last visited Nov. 7, 2022), https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/.

[29] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolensells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[30] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[31] *Id.* at 25.

[32] *Id.*

$11.33 and $16.58 per website.[33] The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[34] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

42. The FTC has also recognized that consumer data is a lucrative (and valuable) form of currency for businesses. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable.[35] Data is currency.[36]

43. When a data breach reveals Sensitive Information, it destroys the privacy and confidentiality of that data. Not only does that upset consumer expectations and wishes, but it also renders the data less valuable in the economy. Sensitive and personal "data has economic value" and can be used to further "artificial intelligence tools as well as the creation of intelligence targeting packages." Indeed, the integrity of Sensitive Information is material to individual's ability to prove their identity, which is necessary for individuals to obtain mortgages, credit cards, business loans; to submit tax returns; and to apply for a job.

44. Consumers, likewise, exchange this type of information to businesses in exchange for goods, services, access, or discounts.

45. When this information is released to cybercriminals and placed on the dark web, then individuals are less able to use that information to prove their identity because that information has been exposed to others willing or able to falsify and steal others' identities. Thus, the value of the breached information is lessened and its usefulness impaired.

---

[33] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Nov. 6, 2022).

[34] *Id.*

[35] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Nov. 7, 2022) https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable.

[36] *Id.*

46. Chegg's failure to provide reasonable data security for its users' Sensitive Information has caused and is likely to continue to cause substantial injury, including but not limited to identity theft, fraud, out-of-pocket monetary losses, decreased value of personal information, and time and effort spent remedying or attempting to prevent injuries, to those individuals whose data was exposed in breaches.

CLASS ALLEGATIONS

47. Plaintiff brings this action on behalf of himself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All individuals whose data was impacted or otherwise compromised by one of, or any combination of the four, Chegg's Data Breaches.

48. Excluded from the class is Chegg and its subsidiaries and affiliates; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

49. Plaintiff reserves the right to, after conducting discovery, modify, expand or amend the above Class definition or to seek certification of a class or Classes defined differently than above before any court determines whether certification is appropriate.

50. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are millions of members of the Class. The number of reportedly impacted individuals already exceeds forty (40) million, and Plaintiff believes additional entities and persons may have been affected by the Data Breaches. The precise number of class members, however, is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

51. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law

and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether Chegg knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether Chegg controlled and took responsibility for protecting Plaintiff's and the Class's data when solicited that data, collected it, and stored it on its servers;

c. Whether Chegg's security measures were reasonable considering the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether Chegg owed Plaintiff and the Class a duty to implement reasonable security measures;

e. Whether Chegg's failure to adequately secure Plaintiff's and the Class's data constitutes a breach of its duty to institute reasonable security measures;

f. Whether Chegg's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiff's and the Class's data;

g. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Chegg's failure to reasonably protect its data systems; and

i. Whether Plaintiff and the Class are entitled to relief.

52. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Class. Plaintiff and the members of the Class are persons whose provided data to Chegg, whose data resided on Chegg's servers, and whose personally identifying information was exposed in Chegg's Data Breaches. Plaintiff's injuries are like other class members and Plaintiff seeks relief consistent with the relief due to the Class.

53. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Chegg to obtain relief for himself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

54. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

55. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

LEGAL CLAIMS

COUNT I

Negligence

56. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

57. Chegg owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class and managed and stored. This duty arises from multiple sources.

58. Chegg owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target Chegg's data systems and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and the Class would be harmed. Chegg alone controlled its technology, infrastructure, and cybersecurity. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. Furthermore, Chegg knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the

consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and the Class, was the foreseeable consequence of Chegg's unsecured, unreasonable data security measures.

59. Additionally, Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Chegg to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Chegg's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Chegg of failing to use reasonable measures to protect sensitive data. Chegg, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Chegg's duty to adequately protect sensitive information. By failing to implement reasonable data security measures, Chegg acted in violation of § 5 of the FTCA.

60. Chegg is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring Chegg to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

61. Finally, Chegg assumed the duty to protect users' sensitive data by soliciting, collecting, and storing users' data and, additionally, by representing to consumers that it "takes commercially reasonable security measures to protect the Personal Information submitted to [it]."

62. Chegg breached its duty to Plaintiff and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. Chegg knew or should have known that hackers might target sensitive data that Chegg solicited and collected on its users and, therefore, needed to use reasonable data security measures to protect against a Data Breach. Indeed, Chegg acknowledged it was subject to certain standards to protect data and utilize other industry standard data security measures. Chegg, furthermore, represented to users that their data was safe with Chegg.

63. Chegg was fully capable of preventing the Data Breach. Chegg, as a smart technology based company, knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. Chegg thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

64. As a direct and proximate result of Chegg's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

COUNT II

Negligence *Per Se*

65. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

66. Chegg's unreasonable data security measures and constitute unfair or deceptive acts or practices in or affecting commerce in violation Section 5 of the FTC Act.[37] Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Chegg failed to do.

67. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Chegg of failing to use reasonable measures to protect users' sensitive data. The FTC's complaint against Chegg also forms the basis of Chegg's duty.[38]

68. Chegg violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Chegg's conduct was particularly unreasonable given the sensitive nature and amount of data it stored on its users and the foreseeable consequences of a Data Breach should Chegg fail to secure its systems.

[37] *In the Matter of CHEGG, INC., a corporation*, *supra* note 6.
[38] *Id.*

69. Chegg's violation of Section 5 of the FTC Act constitutes negligence per se.

70. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

71. As a direct and proximate result of Chegg's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

COUNT III

Violation of the California Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*
(Injunctive Relief Only)

72. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

73. The Consumers Legal Remedies Act ("CLRA") is liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

74. Chegg is a "person" as defined by the CLRA, and it provided "services" as defined under the act. Cal. Civ. Code §§ 1761(b)-(c), 1770.

75. The CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." *Id.* at § 1770(a)(5).

76. Additionally, the CLRA prohibits a defendant who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another." *Id.* at § 1770(a)(7).

77. Plaintiff Keller and the Class members are "consumer[s]" as who were engaged in a "transaction" under the act. *Id.* at §§ 1761(d)-(e), 1770.

78. Chegg's acts and practices were intended to and did result in the sales of services to Plaintiff and the Class members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Plaintiff Keller's and the Classes' sensitive data, which was a direct and proximate cause of the Data Breaches;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breaches;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breaches;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff Keller's and Class members' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Keller's and Class members' sensitive data, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45.

79. Chegg's omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Chegg's data security and ability to protect the confidentiality of consumers' sensitive information that Chegg solicited, collected, and stored.

80. Had Chegg disclosed, rather than concealing, to Plaintiff and class members that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, Chegg would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

81. Instead, Chegg received, maintained, and compiled Plaintiff's and class members' sensitive data as part of the services Chegg provided and for which Plaintiff and class members paid, in part, through transaction fees by (1) omitting and concealing information from Plaintiff Keller and Class members that Chegg's data security practices were knowingly insufficient to maintain the safety and confidentiality of Plaintiff's and class members' sensitive data and (2) that Chegg was not compliant with basic data security requirements and best practices to prevent a Data Breach. Accordingly, Plaintiff

Keller and the Class members acted reasonably in relying on Chegg's omissions, the truth of which they could not have discovered.

82. On November 8, 2022, Plaintiff Keller and the Class sent notice to Chegg in compliance with California Civil Code § 1782(a) via certified mail. Plaintiff and the other members of the Class seek only injunctive relief in this complaint, but will amend this complaint to seek damages if Defendant does not comply with the California Civil Code § 1782(a) notice.

COUNT IV

Violation of the California Civil Code § 1798.150
(Actual Damages and Injunctive Relief Only)

83. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

84. Chegg is a corporation organized or operated for the profit or financial benefit of its owners with annual net revenues over $776.3 million in 2021 and between $830 and $850 million in 2022.[39]

85. Chegg collects and stores consumers personal information, including sensitive and personal information, as defined by Cal. Civ. Code § 1798.81.5.

86. Chegg had a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Keller's and members of the Class's sensitive and personal data.

87. Chegg failed to meet its duty, resulting in unauthorized access and exfiltration, theft, or disclose of Plaintiff Keller's, and the Class's, personal and sensitive data in violation of § 1798.150.

88. Plaintiff Keller and members of the Class seek relief pursuant to § 1798.150(a), including *inter alia*, actual damages, injunctive relief, and any other relief this Court deems proper. Plaintiff Keller and the Class also seek attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5. Plaintiff does not seek statutory damages in this complaint.

89. On November 8, 2022, Plaintiff Keller and the Class sent notice to Chegg in compliance with California Civil Code § 1798.150(b) via certified mail. Plaintiff and the other members of the Class seek only actual damages and injunctive relief in this complaint, but will amend this complaint to seek statutory damages if Defendant does not comply with the California Civil Code § 1798.150(b) notice.

[39] *Chegg Investor Relations*, *supra* note 26.

90. Because Chegg is still in possession of Plaintiff Keller's, and the other members of the Class's, sensitive and personal data, Plaintiff Keller seek injunctive or other equitable relief to ensure that Chegg implements and maintains reasonable data security measures and practices to prevent an event like the Data Breach from occurring again.

COUNT V

Declaratory and Injunctive Relief

91. Plaintiff repeats and re-alleges the foregoing allegations as if fully set forth herein.

92. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

93. An actual controversy has arisen in the wake of the Data Breaches at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Chegg's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

94. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Chegg owed, and continues to owe a legal duty to secure the sensitive information with which it is entrusted, specifically including information it obtains from its customers, and to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act;

b. Chegg breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal information; and

c. Chegg's breach of its legal duty continues to cause harm to Plaintiff and the Class.

95. The Court should also issue corresponding injunctive relief requiring Chegg to employ adequate security protocols consistent with industry standards to protect its users' and employees' (*i.e.*, Plaintiff's and the Class's) data.

96. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Chegg's data systems. If another breach of Chegg's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

97. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Chegg if an injunction is issued.

98. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

99. Wherefore, Plaintiff, on behalf of himself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and their counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest (except for the claim for violation of the CLRA, which only seeks injunctive relief in this complaint, and the claim for violation of section 1798.150 of the California Civil Code, which only seeks actual, but not statutory damages in this complaint);

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs as allowed by law; and

f. An award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

Plaintiff hereby demands a jury trial for all the claims so triable.

Dated: November 8, 2022

REESE LLP

/s/ Michael R. Reese
Michael R. Reese
mreese@reesellp.com
Sue J. Nam
snam@reesellp.com
100 West 93rd Street, 16th Floor
New York, New York 10025
Telephone: (212) 643-0500

REESE LLP
George V. Granade (Cal. State Bar No. 316050)
ggranade@reesellp.com
8484 Wilshire Boulevard, Suite 515
Los Angeles, California 90211
Telephone: (310) 393-0070

ZIMMERMAN REED LLP
Caleb Marker
caleb.marker@zimmreed.com
6420 Wilshire Blvd., Suite 1080
Los Angeles, California 90048
Telephone: (877) 500-8780

ZIMMERMAN REED LLP
Brian C. Gudmundson
bgudmundson@zimmreed.com
Rachel K. Tack
rachel.tack@zimmreed.com
Michael J. Laird
michael.laird@zimmreed.com
1100 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402
Telephone: (612) 341-0400

Counsel for Plaintiff and the Class